IN THE CLAIMS:

Please cancel claims 1-32 without prejudice or disclaimer, and substitute new claims 33-64 therefor as follows:

Claims 1-32 (Cancelled).

33. (New) A process for secure communication over a wireless network including a group of terminals, wherein such terminals exchange information ciphered by means of at least one key, comprising the step of generating said at least one key independently at each said terminal in said group by means of a protocol of the group key agreement type.

34. (New) The process of claim 33, comprising the steps of:

generating, at each said terminal in said group, respective secret local data and maintaining said local data secret at said terminal;

exchanging publicly accessible information among the terminals in said group; and

generating, independently at each said terminal in the group, said at least one key on the basis of said respective local data maintained secret at each said terminal and said publicly accessible information.

35. (New) The process of claim 34, comprising the step of incorporating to said publicly accessible information coded information representative of each terminal in said group, whereby generation of said at least one key is contributed by all the terminals in said group.

36 (New) The process of claim 35, comprising the steps of:

encoding each terminal in said group by means of respective labels; and

generating a vector of the labels of all the terminals in said group, wherein said

vector is included in said publicly accessible information exchanged among the

terminals in said group.

37.   (New) The process of claim 34, wherein publicly accessible information

exchanged among terminals in said group is representative of a tree-structure for

generating said at least one key.

38.   (New) The process of claim 33, comprising the step of generating said at

least one key independently at each said terminal in said group by means of a Diffie-

Hellman group algorithm.

39.   (New) The process of claim 38, wherein said algorithm is the TGDH

algorithm.

40.   (New) The process of claim 33, comprising the step of each terminal in

said group authenticating itself by means of digital authentication information.

41.   (New) The process of claim 40, comprising the step of each terminal in

said group authenticating itself by means of a digital certificate.

42.   (New) The process of claim 34, comprising the step of exchanging said

publicly accessible information by means of information packets.

43.   (New) The process of claim 42, comprising the step of fragmenting said

publicly accessible information over a plurality of information packets.

44.   (New) The process of claim 34, comprising the steps of each terminal in

said group authenticating themselves by means of digital authentication information,

fragmenting said publicly accessible information over a plurality of information packets and associating said authentication information with all of said packets.

45.   (New) The process of claim 34, comprising the steps of each terminal in said group authenticating themselves by means of digital authentication information, fragmenting said publicly accessible information over a plurality of information packets and including said digital authentication information with one of said packets, whereby the remaining part of said plurality of packets comprises a lower protocol layer conveying information resulting from said fragmentation.

46.   (New) The process of claim 33, comprising the step of configuring said each terminal in said group for generating at least one message selected from the group of:

a join message generated when said terminal enters said group and conveying information that merged with other information provided by all the other terminals in said group is adapted to generate said at least one key;

a key message generated during the generation of said at least one key and containing data that respective terminals other than a new terminal joining said group have to provide for generating said at least one key; and

a leave message generated to notify the other terminals in said group that the source terminal is leaving the group.

47.   (New) The process of claim 33, wherein when a new terminal joins said group, it includes the step of selecting one of the other terminals in the group for exchanging said publicly accessible information with said new terminal joining the group.

48.   (New) A wireless network for secure communication among a group of terminals, wherein such terminals exchange information ciphered by means of at least one key, comprising terminals in said group configured for generating said at least one key independently at each terminal by means of a protocol of the group key agreement type.

49.   (New) The network of claim 48, wherein the terminals in said group are configured for:

generating, at each said terminal in said group, respective secret local data and maintaining said local data secret at said terminal;

exchanging publicly accessible information among the terminals in said group; and

generating, independently at each said terminal in the group, said at least one key on the basis of said respective local data maintained secret at each said terminal and said publicly accessible information.

50.   (New) The network of claim 49, wherein the terminals in said group are configured for incorporating to said publicly accessible information coded information representative of each terminal in said group, whereby generation of said at least one key is contributed by all the terminals in said group.

51.   (New) The network of claim 49, wherein the terminals in said group are configured for:

encoding each terminal in said group by means of respective labels; and

generating a vector of the labels of all the terminals in said group, wherein said vector is included in said publicly accessible information exchanged among the terminals in said group.

52.   (New) The network of claim 49, wherein the terminals in said group are configured for exchanging among them publicly accessible information representative of a tree-structure for generating said at least one key.

53.   (New) The network of claim 48, wherein the terminals in said group are configured for generating said at least one key independently at each said terminal in said group by means of a Diffie-Hellman group algorithm.

54.   (New) The network of claim 53, wherein said algorithm is the TGDH algorithm.

55.   (New) The network of claim 48, wherein the terminals in said group are configured for authenticating themselves by means of digital authentication information.

56.   (New) The network of claim 55, wherein the terminals in said group are configured for authenticating themselves by means of a digital certificate.

57.   (New) The network of claim 49, wherein the terminals in said group are configured for exchanging said publicly accessible information by means of information packets.

58.   (New) The network of claim 49, wherein the terminals in said group are configured for fragmenting said publicly accessible information over a plurality of information packets.

59.   (New) The network of claim 49, wherein the terminals in said group are configured for authenticating themselves by means of digital authentication information,

fragmenting said publicly accessible information over a plurality of information packets

and associating said authentication information with all of said packets.

60.   (New) The network of claim 49, wherein the terminals in said group are

configured for authenticating themselves by means of digital authentication information,

fragmenting said publicly accessible information over a plurality of information packets

and including said digital authentication information with one of said packets, whereby

the remaining part of said plurality of packets comprises a lower protocol layer

conveying information resulting from said fragmentation.

61.   (New) The network of claim 48, wherein the terminals in said group are

configured for generating at least one message selected from the group consisting of:

a join message generated when said terminal enters said group and conveying

information that merged with other information provided by all the other terminals in said

group is adapted to generate said at least one key;

a key message generated during the generation of said at least one key and

containing data that respective terminals other than a new terminal joining said group

have to provide for generating said at least one key; and

a leave message generated to notify the other terminals in said group that the

source terminal is leaving the group.

62.   (New) The network of claim 48, wherein the terminals in said group are

configured for selecting, when a new terminal joins said group, one of the other

terminals in the group for exchanging said publicly accessible information with said new

terminal joining the group.

63.   (New) The network of claim 48, comprising a network according to the 802.11 standard.

64.   (New) A computer program product, directly loadable in the memory of at least one computer and including software code portions adapted for implementing the method of any one of claims 33-47.